REMARKS

By this amendment, Applicants have amended the claims to more clearly define their invention. In particular, Applicants have amended claim 1 to recite that the rights management engine, the storage device for storing data and the storage device for recording a time stamped and digitally signed audit trail are in communication with the server. Claim 1 has also been amended to recite that the server, the rights management engine, the storage device for storing the data and the storage device for recording a time stamped and digitally signed audit trail are separate from the at least one user device. See, Figures 1 and 2. Claim 1 has also been amended to recite that the data is rendered by the server. See, e.g., page 6, lines 12 to 24, especially page 6, lines 17-18 of the substitute specification.

Independent claims 6, 13 and 19 have been amended to clarify that the data is rendered by the server. See, e.g., page 6, lines 17-18 of the substitute specification.

Claims 1-3, 6-8, 10-15 and 17-21 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Patent 6,834,110 to The Marconcini et al. Applicants traverse this rejection and request reconsideration thereof.

The present invention relates to a system for communicating data and protecting rights, to a method of communicating data from a server to a wireless user device and protecting rights therein, to a rights secure communication device for wirelessly providing data to a user device, and to a computer program embodied on a computer readable medium and executable by a computer to communicate data having protected rights. For example, the present invention relates to a system for protecting copyrighted materials which are digitally transferred. According to the present invention, at least one user device, e.g., a terminal, is wirelessly connected to a server, digital rights management engine and content storage device. After the user is authenticated, the server gains authorization to forward the content to the user. By having almost all functions in a secure area of the server, illegal copying is less likely to occur.

In order for prior art systems to work, they must either completely trust the end user or must have a terminal with a high level of storage and processing capability in order to handle the special systems, such an encryption, that are necessary. This provides a great disadvantage for wireless devices which must be small and simple in order to keep them inexpensive and portable. See, e.g., page 2, lines 2-5 of Applicants' specification. One aspect of the present invention is to move as much data processing and storage to the server end so that the user's wireless device can be small, simple, inexpensive and portable. For example, the system of the present invention allows for the user to receive and use the data without the decryption occurring in the end user's wireless device. Thus, according to the present invention, the data is rendered by the server.

The Marconcini et al. patent discloses a method of securely providing data to a user's system over a broadcast infrastructure. The method includes the steps of encrypting the data using a first encrypting key; encrypting a first decrypting key using a second encrypting key; dividing at least part of the encrypted data into a series of logical packages; placing at least some of the logical packages into a broadcast carousel for cyclical broadcast over the broadcast infrastructure; broadcasting the packages in broadcast carousel so that they can be received by at least one user's system, wherein the broadcast is cyclical and repeats periodically; and transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key, to the user's system. In another embodiment in Marconcini et al., a system is disclosed to carry out the above method in a broadcast infrastructure and an image overlaid on top of a primary image being displayed issued to denote that additional logical packages are available for receipt by broadcast.

As described at column 14, line 27 et seq of Marconcini et al., the End-User Device(s) 109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCS, set top boxes (IRDs), and Internet appliances. The End-User Player Application 195 could be implemented in software and/or consumer electronics hardware. In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management in the End-User Device(s) 109. The End-User Device(s) 109 manages the download and storage of the SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions in order to process the content's Usage Conditions embedded in the watermark. The terms End-User(s) and End-User Player Application 195 are used throughout Marconcini et al. to mean through the use or running-on an End-User Device(s) 109.

Thus, in The Marconcini et al., the requested data is watermarked, encrypted with a key, and the key is encrypted. In the end-user device, the key is decrypted and, after that, the data is decrypted using that key. Also, every time the data file is managed, the device has to check the information on the watermark if it is allowed to use the data. The Marconcini et al. patent describes exactly what the present invention tries to avoid.

In The Marconcini et al., the end-user's device is expected to be able to handle larger amounts of data storage, e.g. handling of watermarks and encryption keys (and to have the calculation power in the device to do the encryption). On the other hand, according to the present invention, if the end-user's device has the right to download something, the rendering is done completely in the server, so the end-user has only two play/show the data.

In summary, the Marconcini et al. patent does not describe a system, method, communication device or computer program in which <u>the data is rendered by the server</u>, as presently claimed. Accordingly, the Marconcini et al. patent does not anticipate the presently claimed invention.

Claims 4 and 5, claim 16 and claim 9 all stand rejected under 35 U.S.C. 103(a) as being unpatentable over Marconcini et al. in view of U.S. Patent 6,065,110 to Laursen et al. Applicants traverse these rejections and request reconsideration thereof.

The Laursen et al. patent has been cited by the Examiner as allegedly disclosing various features set forth in claims 4, 5, 16 and 9. However, clearly the Laursen et al. patent does not remedy the basic deficiency noted above with respect to Marconcini et al. That is, it would not have been obvious, based on the teachings of Laursen et al., to modify the Marconcini et al. system to render the data by the server. Accordingly, the presently claimed invention is patentable over the proposed combination of Marconcini et al. and Laursen et al.

In view of the foregoing amendments and remarks, favorable reconsideration and allowance of all of the claims now in the application are requested.

To the extent necessary, applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (Case: 0171.38953X00), and please credit any excess fees to such deposit account.

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Alan E. Schiavelli
Registration No. 32,087

AES/at
(703) 312-6600